WEST POMERANIAN UNIVERSITY OF TECHNOLOGY SZCZECIN
FACULTY OF INFORMATICS

M. Sc. Michał Glet

Universal set of indicators for detecting ransomware attacks

Abstract

Ransomware poses a significant security threat to all sectors, including government institutions, businesses, and users, causing extensive financial and operational damage. The paper explores how ransomware impacts various entities and reveals a constant evolution of the malware. Attackers are enhancing their methods through advanced social engineering and exploiting software vulnerabilities. However, there is a positive shift in response; fewer ransomware attacks result in ransom payments, suggesting an increase in public awareness and preventative measures like regular data backups.

The research forecasts that the ransomware sector will continue to evolve due to its profitability, yet the average lifespan of ransomware is decreasing, now about 70 days. This reduction is attributed to more effective responses from antivirus developers and law enforcement, but each new variant can still inflict considerable damage during its activity. This highlights the need for sophisticated detection methods that can quickly identify and mitigate threats from new, unknown versions of ransomware.

In the dissertation, various ransomware samples were analyzed to identify characteristic features and develop novel detection methods based on randomness examination and data categorization. These methods aim to detect active ransomware attacks effectively. The study introduces a set of indicators designed to recognize the activity of newly developed ransomware variants, potentially reducing their operational lifespan. Tests using prototype implementations of these indicators demonstrated their effectiveness, providing promising avenues for enhancing cybersecurity measures against ransomware threats.

Keywords: ransomware, cybersecurity, threat, cryptography, detection, malware.